



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/977,192	10/16/2001	Stefan Andersson	0119-082	3198

42015 7590 10/09/2007
POTOMAC PATENT GROUP PLLC
P. O. BOX 270
FREDERICKSBURG, VA 22404

EXAMINER

WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
----------	--------------

2137

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

10/09/2007

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

tammy@ppglaw.com

Office Action Summary	Application No. 09/977,192	Applicant(s) ANDERSSON, STEFAN	
	Examiner Jeffery Williams	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 June 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19, 24-30 and 32-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19, 24-30 and 32-50 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2137

DETAILED ACTION

Claims 1 – 19, 24 – 30, 32 – 50 are pending.

This action is in response to the communication filed on 6/25/07.

All objections and rejections not set forth below have been withdrawn.

In view of the supplemental appeal brief filed on 6/25/07, PROSECUTION IS
HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the
following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply
under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed
by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and
appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth
in 37 CFR 41.20 have been increased since they were previously paid, then appellant
must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by
signing below:

Drawings

The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the features of claims 7, 8, 15, and 44, essentially – *means for communicating over a wireless interface with a wireless communications network; means for connection to a remote computer without involving the wireless communications network; means for connection to the remote computer comprises a short-range wireless communications transceiver, for sending signals to and receiving signals from the remote computer; wherein the cryptographic module is provided on an external smart card; A mobile communications device, the mobile communications device being able to communicate over a first wireless interface with a telecommunications network, and comprising a cryptographic module to provide cryptographic functionality for use in communications over the first wireless interface –* must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate

changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The amendment filed 7/25/06 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

Applicant adds the following new matter to page 6: *Regardless of whether a wired, or wireless connection is used, those aspects of the connection residing within the mobile phone 30 constitute means for connection to the PC 10 (which is external, and therefore remote from, the mobile phone 30) without involving the wireless communications network that the mobile phone 30 is additionally capable of communicating with.*

Applicant adds the following new matter to page 8:

Art Unit: 2137

1 It will thus be recognized that, as the previously established communication link
2 between the MS 30 and the PC 10 is used for this communication, the MS 30 therefore
3 functions as a cryptographic service provider to the PC 10 for encrypting
4 communications from the PC 10 over the network 12 without the MS 30 sending the
5 encrypted communications over the wireless communications network with which the
6 MS 30 can also communicate.

7 Applicant adds the following new matter to pages 10 and 11:

8 Regardless of whether a wired, or wireless connection is used, those aspects of
9 the connection residing within the mobile phone 30 constitute means for connection to
10 the PC 60 (which is external, and therefore remote from, the mobile phone 30) without
11 involving the wireless communications network that the mobile phone 30 is additionally
12 capable of communicating with.

13 Applicant adds the following new matter to page 12:

14 It will thus be recognized that, as the previously established communication link
15 between the MS 30 and the PC 60 is used for this communication, the MS 30 therefore
16 functions as a cryptographic service provider to the PC 60 performing the requested
17 cryptographic service and returning the results to the PC 60 without the MS 30 sending
18 the encrypted communications over the wireless communications network with which
19 the MS 30 can also communicate.

20 Applicant is required to cancel the new matter in the reply to this Office Action.

21

1 The specification is objected to as failing to provide proper antecedent basis for
2 the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction
3 of the following is required:

4 The specification does not provide antecedent basis for the added limitation "*for*
5 *encrypting said communications from said computer over said computer network*
6 *without sending said encrypted communications over said wireless communications*
7 *network*", claimed within the amended claim 1.

8 The specification does not provide antecedent basis for the added limitation
9 "*means for connection to a remote computer without involving the wireless*
10 *communications network*", claimed within the amended claim 7.

11 The specification does not provide antecedent basis for the added limitation
12 "*allowing the personal computer to communicate encrypted data over said computer*
13 *network without sending data over said wireless communications network*", claimed
14 within the amended claim 19.

15 The specification does not provide antecedent basis for the added limitation
16 "*using the encrypted data in communications over the computer network without*
17 *sending the encrypted data over the wireless communications network*", claimed within
18 the amended claim 28

19 The specification does not provide antecedent basis for the added limitation
20 "*without the mobile communications device sending the encrypted data over the*
21 *telecommunications network*", claimed within the amended claim 36. Furthermore, the
22 specification does not provide antecedent basis for the added limitation "*a computer*

1 *including: ... a mobile communication device including a cryptographic module", claimed*
2 *within the amended claim 36.*

3 The specification does not provide antecedent basis for the added limitation
4 *"without sending the results of the cryptographic function over the first wireless*
5 *interface", claimed within the amended claim 44.*

6
7
8 ***Claim Rejections - 35 USC § 112***

9
10 The following is a quotation of the first paragraph of 35 U.S.C. 112:

11 The specification shall contain a written description of the invention, and of the manner and process of
12 making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the
13 art to which it pertains, or with which it is most nearly connected, to make and use the same and shall
14 set forth the best mode contemplated by the inventor of carrying out his invention.
15

16 **Claims 1 – 19, 28 – 30, and 32 – 46 are rejected under 35 U.S.C. 112, first**
17 **paragraph, as failing to comply with the written description requirement. The**
18 **claim(s) contains subject matter which was not described in the specification in**
19 **such a way as to reasonably convey to one skilled in the relevant art that the**
20 **inventor(s), at the time the application was filed, had possession of the claimed**
21 **invention. See objection to specification.**

22
23 ***Claim Rejections - 35 USC § 101***

24
25 35 U.S.C. 101 reads as follows:

Art Unit: 2137

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 19 and 47 – 50 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Specifically, regarding claims 19 and 47 - 50, the recitations of a realizable or discernable modules are merely recitations of software applications/instructions alone. Computer instructions per se. do not fall within one of the statutory categories of invention. Thus claim 19 is rejected as non-statutory.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 47 and 48 are rejected under 35 U.S.C. 102(b) as being anticipated by Caputo et al., "Pocket Encrypting and Authenticating Communications Device", U.S. Patent 5,778,071.

Regarding claim 47, Caputo et al. discloses:

an application interface for connection to a computer application (2:47-55; 15:25-34); and an external interface for connection to a mobile communication device containing a cryptographic module wherein (2:47-55), when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom (Caputo et al., 15:13-39, 17:12-67; 18:1-9; figs. 3, 4a, 5a). Caputo discloses that the module commands the cryptographic module to encrypt data.

Regarding claim 48, Caputo et al. discloses:

wherein the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function (Caputo et al., Col. 15, lines 13-39).

Caputo discloses a system comprising a module interfaced with a cryptographic module for purposes of providing cryptographic functionality. Computerized modules operate in response to commands and requests, such as sets of instructions, codes, or signals. Consequently, the module comprises means to provide the requested cryptographic function (establish that it is capable of providing the requested cryptographic function).

Art Unit: 2137

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 4, 6, 7, 11, 13 – 15, 18, 19, 24, 26 – 28, 32 – 34, 36 – 39, 42, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo et al. (Caputo), "Pocket Encrypting and Authenticating Communications Device", U.S. Patent 5,778,071 in view of Liebenow et al. (Liebenow), "Dual Mode Modem for Automatically Selecting Between Wireless and Wire-based Communication Modes", U.S. Patent 6,131,136.

Regarding claim 1, Caputo et al. discloses a method of authenticating communications, the method comprising:

initiating communications from said computer over a computer network; determining that encryption of said communications is required; establishing a connection with a mobile communications device, wherein said mobile communications device includes a cryptographic module for use in mobile communication (Caputo, fig. 3; 9:46-60; 15:13-39).

using the cryptographic module of the mobile communications device as an cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network (Caputo, fig. 3; 9:46-60; 15:13-39; 2:23-27; 3:33-38).

1 Caputo discloses a mobile communications device with a modem. The modem
2 is shown to connect to a wired communications network (Caputo, fig. 3). Caputo does
3 not disclose that the mobile communication device is also usable over a wireless
4 communications network.

5 Liebenow discloses that mobile communication devices should possess modems
6 with the ability to communicate via both wired and wireless communications networks.
7 Liebenow discloses that such an arrangement offers mobile communication devices the
8 flexibility and convenience to communicate with whichever type of network is available
9 and further protects the mobile communications device from the misuse of power
10 (Liebenow, Abstract, 1:13-26; 1:65 – 2:5).

11 It would have been obvious to one of ordinary skill in the art to employ the dual
12 modem features of Liebenow within the mobile communication device of Caputo. This
13 would have been obvious because one of ordinary skill in the art would have been
14 motivated by benefits taught by Liebenow.

15 Thus, the combination of Caputo and Liebenow disclose:
16 *over a wireless communications network* (Caputo, fig. 4a:40; Liebenow, fig. 1).

17
18 Regarding claim 4, the combination of Caputo and Liebenow disclose:
19 *wherein the step of establishing a connection with the mobile communications*
20 *device comprises establishing a wired connection between the mobile communications*
21 *device and the computer* (Caputo; fig. 3).

22

Art Unit: 2137

1 Regarding claim 6, the combination of Caputo and Liebenow disclose:

2 *when the application program interface requires cryptographic functionality,*
3 *calling a cryptographic service provider function in the mobile communications device*
4 *(Caputo, 15:13-39).*

5
6 Regarding claim 7, it is rejected, at least, for the same reasons as claim 1, and
7 furthermore because the combination of the combination of Caputo, Liebenow, and
8 Geiger disclose:

9 *means for communicating over a wireless interface with a wireless*
10 *communications network (Caputo, fig. 4a:40; Liebenow, fig. 1);*

11 *means for connection to a remote computer without involving the wireless*
12 *communications network (Caputo, fig. 3);*

13 *and a cryptographic module, the cryptographic module being usable: for*
14 *encoding wireless communications from the device over said wireless interface; by a*
15 *cryptographic service provider with an application program interface of the remote*
16 *computer (Caputo et al., Col. 2, lines 23-27; Col. 3, lines 33-38, 46-50; Col. 15, lines 13-*
17 *39, figs. 2, 3, 4a, 5a; Liebenow, fig. 1).*

18
19 Regarding claim 11, the combination of the combination of Caputo and Liebenow
20 disclose:

21 *wherein the cryptographic module uses public key cryptography (Caputo et al.,*
22 *Col. 1, lines 27-39; Col. 11, lines 18-59).*

1
2 Regarding claim 18, the combination of the combination of Caputo and Liebenow
3 disclose:

4 *an interface for receiving a command from a personal computer, the mobile*
5 *communications device acting as a cryptographic service provider for said personal*
6 *computer in response to said command* (Caputo et al., Col. 15, lines 13-39).
7

8 Regarding claim 19, it is rejected, at least, for the same reasons as claim 1, and
9 furthermore because the combination of Caputo et al. and Liebenow disclose:

10 *a tangible module for a personal computer, wherein, in response to the module*
11 *receiving a first command from a cryptographic application program interface, indicating*
12 *that it requires cryptographic functionality for communication over a computer network,*
13 *the module sends a second command to a mobile communication device, the mobile*
14 *communication device having a cryptographic module for use in mobile communication*
15 *over a wireless communications network, such that the cryptographic module acts as a*
16 *cryptographic service provider for said personal computer allowing the personal*
17 *computer to communicate encrypted data over said computer network without sending*
18 *data over said wireless communications network* (Liebenow, fig. 1; Caputo, fig. 3; 15:13-
19 39; 17:12-67; 18:1-9). The combination of Caputo and Liebenow disclose a system
20 comprising an application program running on a computer, the application being
21 interfaced with a cryptographic module for purposes of providing cryptographic
22 functionality. Computer applications, as well as the cryptographic module, operate

1 using commands, such as sets of instructions, codes, or signals. When the application
2 is instructed to utilize the cryptographic module, commands are sent to enable such
3 usage.

4
5 Regarding claim 24, it is rejected, at least, for the same reasons as claim 1, and
6 furthermore because the combination of Caputo and Liebenow disclose:

7 *a computer; and mobile communications device, including a cryptographic*
8 *module for performing cryptographic functions in mobile communication over a wireless*
9 *communications network, the computer having at least one application which requires*
10 *cryptographic functionality for communication over a computer network, a first part of*
11 *the required cryptographic functionality being provided in the computer; and a second*
12 *part of the required cryptographic functionality being provided in the mobile*
13 *communications device* (Liebenow, fig. 1; Caputo 15:13-39, col. 9, lines 28-36). As
14 disclosed, each of the computer and the mobile communications device cooperate to
15 provide the resulting cryptographic functionality. Thus, the computer and the mobile
16 device provide first and second parts of cryptographic functionality. Additionally, the
17 computer provides instructions for the operation of the encrypting device, including
18 functionality for the manipulation of encryption modes, and combining unencrypted data
19 with encrypted data to submission to further encryption processing. The device
20 executes an encryption algorithm for encrypting the data submitted by the computer.
21 *the computer and the mobile communications device having means for*
22 *establishing a secure communications path there between* (Caputo et al., fig. 3); and the

1 *computer further comprising an interface device which, on determining that an*
2 *application needs use cryptographic functionality, selects the functionality provided in*
3 *the computer, or the functionality provided in the mobile communications device, and*
4 *sends command thereto (Caputo et al., Col. 15, lines 13-39).*

5
6 Regarding claim 26, Caputo et al. discloses:
7 *wherein the computer application which requires cryptographic functionality is an*
8 *internal memory access application (Caputo et al., Col. 15, lines 13-39).*

9
10 Regarding claim 27, Caputo et al. discloses:
11 *wherein the computer application which requires cryptographic functionality is an*
12 *external communication application (Caputo et al., Col. 15, lines 13-39).*

13
14 Regarding claims 28, it is rejected, at least, for the same reasons as claim 1, and
15 furthermore because the combination of Caputo and Liebenow disclose:

16 *sending data to be encrypted from the computer to a mobile communications*
17 *device, wherein the mobile communications device has a cryptographic module for*
18 *performing cryptographic functions in communications over a wireless communications*
19 *network, and further, wherein the mobile communications device uses the cryptographic*
20 *module to encrypt the data (Caputo, fig. 3; 9:46-60; 15:13-39; 2:23-27; 3:33-38);*
21 *receiving the encrypted data at the computer from the mobile communications*
22 *device (Caputo, 15:13-39);*

1 *and using the encrypted data in communications over the computer network*
2 *without sending the encrypted data over the wireless communications network (Caputo,*
3 *fig. 3; 15:13-39).*

4
5 Regarding claims 32 and 33, the combination of Caputo and Liebenow discloses:
6 *using a cryptographic module realized in hardware in the mobile communications*
7 *device and using a cryptographic module realized in software in the mobile*
8 *communications device (Caputo et al., Col. 9, lines 40-45).*

9
10 Regarding claims 34, the combination of Caputo and Liebenow discloses:
11 *using a cryptographic module provided on an external smart card which can be*
12 *read by the mobile communications device (Caputo et. al., Col. 10, lines 19-31, 51-59;*
13 *Col. 13, lines 4-10, 25-67).*

14
15 Regarding claims 13, 14, and 15, they are substantially similar to claims 32, 33,
16 and 34 and they are rejected, at least, for the same reasons.

17
18 Regarding claim 36, it is rejected, at least for the same reasons as claim 1, and
19 furthermore because the combination Caputo and Liebenow disclose:

20 *a computer including: a cryptographic application program interface; and a*
21 *cryptography service provider; and a mobile communication device including, wherein,*
22 *when the cryptographic application program interface determines that the application*

1 *requires cryptographic functionality for communication over a computer network, the*
2 *cryptographic application program interface, sends a command to the cryptography*
3 *service provider (Caputo et al., Col. 15, lines 13-39), and wherein the cryptography*
4 *service provider has a communications link to the cryptographic module of the mobile*
5 *communications device, the cryptographic module of the mobile communications device*
6 *being usable to encrypt communications between the mobile communications device*
7 *and a telecommunications network over a wireless interface (Caputo et al., fig. 3:*
8 *Liebenow, fig. 1), and wherein the cryptography service provider can obtain the*
9 *cryptographic functionality, required by the application, from the cryptographic module*
10 *of the mobile communications device (Caputo et al., Col. 2, lines 23-27; Col. 3, lines 33-*
11 *38) without the mobile communications device sending the encrypted communications*
12 *over the telecommunications network (Caputo, 15:13-39).*

13
14 Regarding claims 37, 38, 39, they are substantially similar to claims 32, 33, and
15 34 and they are rejected, at least, for the same reasons.

16
17 Regarding claim 42, the combination of Caputo and Liebenow discloses:

18 *wherein the cryptography service provider has some cryptographic functionality*
19 *(Caputo, 15:13-39),*

20 *and, on receipt of a command from the cryptographic application program*
21 *interface, determines whether it can perform the required cryptographic functionality, or*
22 *whether to obtain the required cryptographic functionality from the cryptographic module*

1 *of the mobile communications device (Caputo 15:13-39). Caputo discloses a system*
2 *comprising a module interfaced with a cryptographic module for purposes of providing*
3 *cryptographic functionality. Computerized modules operate in response to commands*
4 *and requests, such as sets of instructions, codes, or signals. Consequently, the module*
5 *comprises means to provide the requested cryptographic function (establish that it is*
6 *capable of providing the requested cryptographic function).*

7
8 Regarding claim 44, it is rejected, at least, for the same reasons as claim 1, and
9 furthermore because the combination of Caputo and Liebenow disclose:

10 *the mobile communications device being able to communicate over a first*
11 *wireless interface with a telecommunications network, and comprising a cryptographic*
12 *module to provide cryptographic functionality for use in communications over the first*
13 *wireless interface (Caputo, fig. 3; Liebenow, fig. 1), the mobile communications device*
14 *further comprising a security manager module for receiving commands from a computer*
15 *system over a second interface (Caputo, fig. 2), wherein, in response to suitable*
16 *commands received from the computer system over the second interface, the security*
17 *manager module requests a cryptographic function from the cryptographic module, and*
18 *returns the results of the cryptographic function to the computer system over the second*
19 *interface, without sending the results of the cryptographic function over the first wireless*
20 *interface (Caputo et al., Col. 15, lines 13-39).*

21

1 **Claims 5, 8, 9, 41, and 46 are rejected under 35 U.S.C. 103(a) as being**
2 **unpatentable over the combination of Caputo and Liebenow in view of Ericsson,**
3 **“Bluetooth – A Global Specification for Wireless Connectivity”.**
4

5 Regarding claims 5, 8, 9, 41, and 46, the combination of Caputo and Liebenow
6 disclose a wired connection between the device and the computer (Caputo et al., Col. 6,
7 lines 41-61). The combination does not disclose a wireless connection or connection
8 via a short-range transceiver incorporating Bluetooth wireless technology.

9 Ericsson discloses the obvious use of wireless connections between devices
10 (Ericsson, Page 1). Bluetooth, a short-range radio technology allows for the
11 replacement of wired connections – “facilitating protected” wireless connections
12 between mobile devices. As disclosed, Bluetooth technology can be used to replace
13 “the cumbersome cable used today to connect a laptop to a cellular telephone”.

14 It would be obvious to one of ordinary skill in the art to employ the secure feature
15 of wireless short-range radio connection and Bluetooth technology of Ericsson with the
16 combination of Caputo and Liebenow because it is apparent that the ability to securely
17 operate wirelessly would enhance a security/communication device designed to be
18 mobile and portable.

19
20 **Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over**
21 **Caputo in view of Ericsson, “Bluetooth – A Global Specification for Wireless**
22 **Connectivity”.**

1 Regarding claim 49, Caputo discloses a wired connection between the device
2 and the computer (Caputo et al., Col. 6, lines 41-61). Caputo does not disclose a
3 wireless connection or connection via a short-range transceiver incorporating Bluetooth
4 wireless technology.

5 Ericsson discloses the obvious use of wireless connections between devices
6 (Ericsson, Page 1). Bluetooth, a short-range radio technology allows for the
7 replacement of wired connections – “facilitating protected” wireless connections
8 between mobile devices. As disclosed, Bluetooth technology can be used to replace
9 “the cumbersome cable used today to connect a laptop to a cellular telephone”.

10 It would be obvious to one of ordinary skill in the art to employ the secure feature
11 of wireless short-range radio connection and Bluetooth technology of Ericsson within
12 the system of Caputo because it is apparent that the ability to securely operate
13 wirelessly would enhance a security/communication device designed to be mobile and
14 portable.

15
16
17 **Claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40, are rejected under 35**
18 **U.S.C. 103(a) as being unpatentable over the combination of Caputo and**
19 **Liebenow in view of Geiger et al. (Geiger), “Secure Wireless Electronic-Commerce**
20 **System with Wireless Network Domain”, U.S. Patent 6,463,534 B1.**

21

1 The combination of Caputo and Liebenow disclose a mobile communications
2 device, comprising a cryptographic module, which is used as a token for authenticating
3 a user and for encrypting communications (Caputo, 2:23-27; 3:33-38, 46-50; Fig. 2).
4 The device sends communications to a recipient by wired telephonic means or wireless
5 telephonic means (Caputo, Fig. 2:14; 16:40-45; 17:3-7; Liebenow, fig. 1). The
6 combination of Caputo and Liebenow, however, does not disclose that the wireless
7 mobile communications device is enabled to use the enhanced wireless security of the
8 Wireless Application Protocol.

9 Geiger et al., discloses a wireless mobile device and system used to send secure
10 wireless communication using the Wireless Application Protocol (Geiger, 2:49-65; 9:22-
11 53; 11:64 – 12:8). As disclosed by Geiger et al., WAP (utilizing WTLS and a WIM) is a
12 convenient protocol to use with wireless mobile communications, chosen for its security.

13 Thus, it would have been obvious to one of ordinary skill in the art to employ the
14 secure Wireless Application Protocol feature of Geiger et al. with the combination of
15 Caputo and Liebenow because it is obvious that a wireless mobile communication
16 device designed for authenticated and encrypted communications would be enhanced
17 by the use of a convenient communication protocol and system that features increased
18 wireless security.

19
20 Regarding claim 2, the combination of Caputo, Liebenow, and Geiger disclose:

1 *the mobile communications device is a WAP-enabled device* (Geiger et al., Fig.
2 1, Col. 9, lines 22-53). As disclosed, the device is WAP-enabled since it communicates
3 using the WAP protocol.

4
5 Regarding claim 3, the combination of Caputo, Liebenow, and Geiger disclose:
6 *wherein the cryptographic module is that used by the mobile communications*
7 *device for Wireless Transport Layer Security communications* (Geiger et al., Col. 2,
8 lines 49-65; Col. 6, lines 55-58; Col. 9, lines 22-53). As disclosed, communication
9 security, the functionality provided by the cryptographic module, is accomplished using
10 WTLS communications.

11
12 Regarding claim 10, it is substantially similar to claim 3, and is rejected for the
13 same reasons.

14
15 Regarding claim 12, the combination of the combination of Caputo, Liebenow,
16 and Geiger disclose:
17 *means for sending and transmitting data using WAP* (Geiger et al., Fig. 1, Col. 9,
18 lines 22-53).

19
20 Regarding claims 16 and 17, the combination of the combination of Caputo,
21 Liebenow, and Geiger disclose:

1 *wherein the cryptographic module comprises a Wireless Identity Module card*
2 *and wherein the cryptographic module comprises a Wireless Identity Module card which*
3 *allows communications using Wireless Transport Layer Security. (Geiger et al., col. 11,*
4 *line 64 – col. 12, line 8; fig. 4, elems. 450, 452).*

5
6 Regarding claims 25, 29, and 30, they are substantially similar to claims 2 and 3,
7 and they are rejected for the same reasons.

8
9 Regarding claims 35 and 40, they are substantially similar to claims 16, and are
10 rejected, at least, for the same reasons.

11
12 **Claims 43 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable**
13 **over the combination of Caputo and Liebenow in view of RSA, “PKCS #11 v2.10:**
14 **Cryptographic Token Interface Standard”.**

15
16 Regarding claims 43 and 45, the combination of Caputo and Liebenow discloses
17 a portable encryption and authentication device. The device utilizes a modem and
18 “industry compatible” modem commands for communication (Caputo, 2:160; 17:12-35;
19 16:40-61). The combination, however, does not disclose specifically that the mobile
20 communications device utilizes PKCS #11 with AT commands.

21 RSA discloses that the PKCS #11 command set is the industry standard for
22 encryption and authentication devices (RSA, pages 1-12).

1 It would have been obvious to one of ordinary skill in the art to employ PKCS #11
2 command set, disclosed by RSA to be the industry standard, in the combination of
3 Caputo, Liebenow, and Geiger. This would have been obvious because one of ordinary
4 skill in the art would have been motivated for the purpose of utility and compatibility to
5 utilize the standards defined by industry. Furthermore, the disclosure of AT commands
6 is obvious as these are the standard industry commands used to communicate via
7 modems, as evidenced by the definitions of "AT Command Set" and "Modem
8 Standards" in Newton's Telecom Dictionary, 13th ed.

9
10 **Claim 50 is rejected under 35 U.S.C. 103(a) as being unpatentable over**
11 **Caputo in view of RSA, "PKCS #11 v2.10: Cryptographic Token Interface**
12 **Standard".**

13
14 Regarding claim 50, Caputo discloses a portable encryption and authentication
15 device. The device utilizes a modem and "industry compatible" modem commands for
16 communication (Caputo, 2:160; 17:12-35; 16:40-61). Caputo, however, does not
17 disclose specifically that the mobile communications device utilizes PKCS #11 with AT
18 commands.

19 RSA discloses that the PKCS #11 command set is the industry standard for
20 encryption and authentication devices (RSA, pages 1-12).

21 It would have been obvious to one of ordinary skill in the art to employ PKCS #11
22 command set, disclosed by RSA to be the industry standard, in the system of Caputo.

Art Unit: 2137

1 This would have been obvious because one of ordinary skill in the art would have been
2 motivated for the purpose of utility and compatibility to utilize the standards defined by
3 industry. Furthermore, the disclosure of AT commands is obvious as these are the
4 standard industry commands used to communicate via modems, as evidenced by the
5 definitions of "AT Command Set" and "Modem Standards" in Newton's Telecom
6 Dictionary, 13th ed.

8 ***Response to Arguments***

9
10 Applicant's arguments filed 6/25/07 have been fully considered but they are not
11 persuasive.

12
13 Applicant's argue primarily that:

14 (i) *Argument 1: The specification provides proper antecedent basis for claimed*
15 *subject matter* (Remarks, pg. 10)

16
17 In response the examiner respectfully points out that the added paragraphs to
18 the specification are not supported within the applicant's original disclosure, and
19 therefore, the similar recitations added to the claims are not supported either.

20
21 (ii) *Argument 2: Prior art does not show a division of cryptographic functionality.*
22

Art Unit: 2137

1 In response, the examiner points out that the prior art shows separate elements
2 in cooperation for the provision of cryptographic functionality. Thus the elements
3 provide cryptographic functionality (See above rejections). For example the mobile
4 device can transform data via an encryption algorithm whereas the a computer can
5 construct encrypted messages (Caputo, 15:15-40).

6
7 (iii) Argument 3: The prior art combination does not disclose the claimed features
8 (Remarks, pgs. 16 – 22).

9
10 In response to applicant's arguments (A – C, E) against the references
11 individually, one cannot show nonobviousness by attacking references individually
12 where the rejections are based on combinations of references. See *In re Keller*, 642
13 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231
14 USPQ 375 (Fed. Cir. 1986).

15 In response to argument (D), the examiner points out that it is unpersuasive for
16 the same reasons noted regarding argument 2.

17 Regarding argument (F), the examiner respectfully notes that prior art clearly
18 discloses a mobile device utilized for communications, thus a "mobile communications
19 device" (Caputo, fig. 2).

20
21 (iii) Arguments 4 - 8: The prior art combination does not disclose the claimed
22 features (Remarks, pgs. 22-24).

Art Unit: 2137

1
2 In response to applicant's arguments (A – C, E) against the references
3 individually, one cannot show nonobviousness by attacking references individually
4 where the rejections are based on combinations of references. See *In re Keller*, 642
5 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231
6 USPQ 375 (Fed. Cir. 1986).

7 8 9 Conclusion

10
11 The following prior art made of record and not relied upon is considered pertinent
12 to applicant's disclosure.

13 ***See Notice of References Cited.***

14
15 A shortened statutory period for reply is set to expire 3 months (not less than 90
16 days) from the mailing date of this communication.

17 Any inquiry concerning this communication or earlier communications from the
18 examiner should be directed to Jeffery Williams whose telephone number is (571) 272-
19 7965. The examiner can normally be reached on 8:30-5:00.

20 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
21 supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

Art Unit: 2137

1 number for the organization where this application or proceeding is assigned is (703)

2 872-9306.

3 Information regarding the status of an application may be obtained from the

4 Patent Application Information Retrieval (PAIR) system. Status information for

5 published applications may be obtained from either Private PAIR or Public PAIR.

6 Status information for unpublished applications is available through Private PAIR only.

7 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should

8 you have questions on access to the Private PAIR system, contact the Electronic

9 Business Center (EBC) at 866-217-9197 (toll-free).

10

11 Jeffery Williams

12 Art Unit 2137

13

JW

Cynthia Britt
CYNTHIA BRITT
PRIMARY EXAMINER